UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/828,559	04/06/2001	Osamu Shibata	29288.0300	6490

20322 7590 08/19/2008

SNELL & WILMER L.L.P. (Main)
400 EAST VAN BUREN
ONE ARIZONA CENTER
PHOENIX, AZ 85004-2202

EXAMINER	
HOMAYOUNMEHR, FARID	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
08/19/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/828,559	SHIBATA ET AL.	
	Examiner	Art Unit	
	Farid Homayounmehr	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 April 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-50* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date. _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____

DETAILED ACTION

1. This action is responsive to amendments filed 4/22/08, the application filed 4/6/2001.

2. Claims 1-50 are pending in the case.

Response to Arguments

3. Rejection under section 112, second paragraph:

The rejection is withdrawn due to amendments by the applicant.

4. Rejection under section 112, first paragraph:

Regarding the rejection reflected in the last Office Action section 7.1, Applicant's amendment overcomes the rejection.

Regarding the rejection reflected in the last Office Action section 7.2, applicant's argument is found non persuasive, and the rejection is maintained. Applicant argues that since the Specification does not describe any instance of encrypting the contents decryption key, it discloses a particular requirement of "content decryption key is not required to be encrypted or decrypted". Applicant also

argues that each instance of encryption or decryption has an associated element to perform such encryption or decryption, and since there is no element introduced to perform decryption or encryption on the content encryption key, the Specification supports the limitation. However, this reasoning is unacceptable. If the Specification does not include a certain feature, it does not automatically support the opposite of that certain feature. In other words, if the Specification does not show encryption of content decryption key, it doesn't mean that it supports the requirement of "the content decryption key is not required to be encrypted". The mentioned limitation is a critical element of applicant's argument to distinguish applicant's invention form prior art. The limitation at hand is a negative requirement, added after the original presentation. It must be clearly and explicitly supported by the Specification.

In addition, applicant argues that the content key is never transferred. However, the content encryption/decryption keys are generated based on the decryption limitations. The decryption limitations are encrypted and transferred. Therefore, the elements of the content encryption/decryption key are encrypted and transferred. Therefore, Examiner's concern about how the decryption key is transferred without any encryption in valid.

Based on the discussion above, applicant's argument regarding the rejection reflected in the last Office Action section 7.2 is found non persuasive.

Regarding the rejection reflected in the last Office Action section 7.3, applicant states that the cited feature was well-known in the art, and accordingly there is no need for explicit disclosure. Therefore said feature is considered to be disclosed in prior art and the associated rejection is withdrawn.

5. Rejection under section 103(a):

Applicant argues that Ishibashi requires encrypting the content encryption/decryption key and therefore does not teach the requirement of not encrypting/decrypting the content decryption key. Applicant argues that Examiner admits to such deficiency. There is no such inefficiency. The claim language requires "no encryption/decryption required by the decryption device". As indicated in the rejection, Ishibashi's decryption device that performs decryption of the content (equivalent to applicant's content decryption device) does not decrypt the keys. Therefore, Ishibashi meets the claim requirements, and there is no deficiency.

In addition, Ishibashi clearly teaches the generation of the keys by the encryption and decryption devices. As mentioned previously, applicant's key generation depends on certain elements (decryption limits) to generate the keys, and those elements are encrypted, transferred and decrypted. Ishibashi teaches the same, therefore, if generation of the keys at the device is the reason the keys don't

need encryption or transfer, the same applies to Ishibashi's invention, as it also teaches transferring key elements and generating the key at the device.

Applicants argue again that their invention does not require encryption or decryption, however, as stated previously, the elements of applicants key are encrypted and decrypted prior to generation of the key. If the final generated key is considered not encrypted/decrypted, the same applies to Ishibashi's key, because after Ishibashi's final key is generated it does not require encryption or decryption.

Applicant further argues that Examiner has provided no support for cooperation between server side 10 and the user side 100. However, Ishibashi invention is about controlling the number of copies made available to the user (see col. 1 lines 22-58). It also shows user is charged based on the copies purchased and the profits are shared with the content provider which provides the content. Therefore there is certain cooperation among elements of Ishibashi's system including the user side 100 and the content provider 10.

Applicant further argues that information processor 100 does not generate a content encryption key, however, Fig 8 items 133 and 131 clearly indicate an element performing content key encryption, which generates the content encryption key. Applicant also state that Ishibashi col. 8 lines 8-11 shows that Ishibashi teaches away from generating content encryption key. However, the

cited potion states that the key is stored in a data storage medium. This does not teach away from generation of a key to be used to decrypt the content.

Applicant's argument relative to other pending claims is base on the similar features of claim 1. Accordingly, applicant's argument is found non persuasive.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7. Claims 1-50 rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

7.1. The limitation of "wherein the contents decryption key is not required to be encrypted or decrypted by the decryption device" is introduced, however, there is no definition or description of the said limitation in the Specification.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claim 1 rejected under 35 U.S.C. 103(a) as being unpatentable over Ishibashi (U.S. Patent No. 6,728,379 B1, filed July 28, 1999).

9.1. As per claim 1, Ishibashi is directed to a copyright protection system (column 1 line 22 to 25) comprising: an encryption device (item 10 and associated text. Items 100 and 200 also perform encryption) and a decryption device (Information Processors 100 and 200 both perform decryption, e.g. item 136), wherein cryptographic communication is performed between the encryption device and the decryption device (Figures 2 and 3 and the associated texts) using a key (Kce and Kcd as shown in Figures and associated text. Also note that public key encryption, (which uses separate keys for encryption and decryption) can be replaced by private (symmetric) key encryption, which uses one key for both encryption and decryption, as indicated in col. 4 line 34 to 42), wherein the encryption device includes a contents storage section for storing contents (item 11 of Fig. 8 and associated text), a first contents key generation section for generating the contents key (item 14 of Fig. 8 and associated text, also see column 4 line 24 to 33) based on a second decryption limitation

obtained by updating a first decryption limitation (column 6 line 1 to 20 discloses SCMS as an example system of a copy control scheme that uses control codes in set in the content and the associated encryption keys for copy control. Also note that the process of updating the content key based on the copy control code and client usage and purchase of content is clearly disclosed in col. 9 line 52 to col. 13 line 60. The process is explained within item 100, but it would have been obvious to a person skilled in art to perform the same in item 10 (content provider), where the content key is generated. The motivation is to allow the content provider to control the copying of the content), and a first encryption section for encrypting the contents using the contents key (item 13 Fig. 8) and outputting the encrypted contents (item 15 Fig. 8), and wherein the decryption device includes a second contents key generation section for generating the contents key from the second decryption limitation (item 131 of Fig. 8 generates Kcd, which is used to decrypt the content. As the content was encrypted based on a copy control scheme, namely SCMS, the copy control code was updated and embedded in the content or the key (see column 10 line 53 to 66 and also column 13 line 47 to 60), accordingly) and a first decryption section for decrypting the encrypted contents using the contents key generated by the second contents key generation section (item 136 of Fig. 8 and associated text), wherein the contents decryption key is not required to be encrypted or decrypted by the decryption device (per Fig, 8, item 136 is different from item 131), wherein the encryption device further includes a third encryption section for encrypting the first decryption limitation using a time-varying key and outputting the second

encrypted decryption limitation to the decryption device (the copy control data (encryption limitation) is buried in content data (see, for example, col. 1 line 1-5), and all the communication between devices is encrypted by a session key (see, for example, col. 9 line 3-10, or col. 10 line 60 to col. 13 line 47), which is a time-varying key), and the contents decryption device further includes a third decryption section for decrypting the second encrypted decryption limitation transferred from the third encryption section using the time-varying key and outputting the first decryption limitation (all communication is encrypted by a session key as explained above. Also see Fig. 6 and associated text).

10. Claims 2-50 rejected under 35 U.S.C. 103(a) as being unpatentable over Ishibashi (U.S. Patent No. 6,728,379 B1, filed July 28, 1999), and further in view of Frutiger (US Patent No. 4'071'693, dated 1/31/1978).

10.1. As per claim 2, Ishibashi is directed to a copyright protection system according to claim 1, wherein the decryption device further includes a decryption limitation updating section for updating the first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule (column 12 line 4 to 15), and a second encryption section for encrypting the second decryption limitation using a time-varying key (column 12 line 33 to 43), and outputting the first encrypted decryption limitation, wherein the encryption device further includes a second decryption section for decrypting the first

encrypted decryption limitation transferred from the second encryption section using the time-varying key to generate the second decryption limitation, wherein the first contents key generation section generates the contents key based on the second decryption limitation generated by the second decryption section (column 13 line 15 to 26. Note that the Content provider and the information system 100 also perform the SCMS method for inclusion of the copy control code to limit number of allowable copies at item 100. Therefore, content encryption and key generation at the content provider also involves updating encryption keys based on the control code and in accordance with the copy rights updated at the information center).

Ishibashi teaches a time-varying key that is transmitted between the sender and the receiver, however, it does not explicitly teach time varying keys that are not transmitted between the two parties. Frutiger teaches time-varying keys generated at the receiver and transmitter, and used to generate keys used for encryption/decryption (see the abstract and columns 1 and 2). Ishibashi and Frutiger are analogous art as they are both directed to systems for secure transmission of data. At the time of invention, it would have been obvious to the one skilled in art to combine the method of key generation as taught by Frutiger, in the system of Ishibashi, to include time varying keys in its method of secure delivery of data. The motivation to do so would be to improve the security of key exchange between the receiver and transmitter, which is a critical element of all security systems relying on encryption and decryption keys.

10.2. As per claim 3, Ishibashi is directed to a copyright protection system according to claim 2, wherein the encryption device further includes a first common key storage section for storing a common key (column 9 line 4 to 10 discloses a mutual authentication between all elements in Fig. 8. Furthermore, the said mutual authentication is described in column 7 lines 33 to 65. Therefore, the content provider executes a mutual authentication method, namely ISO/IEC 9798-3, which will require establishment of a common key, and a location for storage), a decryption limitation storage section for storing the first decryption limitation (as described in response to claim 2, the content provider performs SCMS in association with the item 100 to establish a copy code, and therefore stores a copy code, which is updated in sync with item 100), a first random number generation section for generating a first random number, a first mutual authentication section for performing mutual authentication in association with the decryption device using the first random number, and a second random number transferred from the decryption device, a first time-varying key generation section for generating the time-varying key using the first random number and the second random number in response to the authentication by the first mutual authentication section (random number generation and exchange between two parties performing mutual authentication, and establishment of a session key, are part of a mutual authentication method, namely ISO/IEC 9798-3 performed between the content provider and item 100, as described in Fig. 6 and the associated text, and also column 5 lines 5 to 21), and wherein the decryption

device further includes a second common key storage section for storing the common key, a second random number generation section for generating the second random number, a second mutual authentication section for performing mutual authentication in association with the encryption device using the second random number and the first random number, a second time-varying key generation section for generating the time-varying key using the second random number and the first random number in response to the authentication by the second mutual authentication section (again, item 100 performs SCMS for receiving the copy codes using a session key obtained thorough a mutual authentication).

10.3. As per claims 4 and 5 Ishibashi is directed to a copyright protection system according to claim 1, wherein the decryption device further includes a first decryption limitation updating section for updating the first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule (column 6 lines 1 to 20), and a second contents key generation section for generating the contents key based on the second decryption limitation updated by the first decryption limitation updating section (column 10 line 42 to column 11 line 9), wherein the encryption device further includes a second decryption limitation updating section for updating the first decryption limitation to the second decryption limitation in accordance with the decryption limitation updating rule in response to the updating of the first decryption limitation by the first decryption limitation updating section, the first

contents key generation section generates the key based on the second decryption limitation updated by the first decryption limitation updating section (the content provider and Information Processing Unit 200 both perform SCMS and implement copy code updating and secure exchange of the copy code).

10.4. As per claim 6, Ishibashi is directed to a copyright protection system according to claim 5, wherein the second decryption limitation updating section updates the first decryption limitation to the second decryption limitation in advance (column 10 lines 9 to 26 discloses the case when the content decryption and distribution decryption keys are supplied by the Key Distribution Center, item 30, and therefore are supplied in advanced), the first contents key generation section generates the contents key from the second decryption limitation, and the second decryption limitation updating section stores the second decryption limitation in the decryption limitation storage section in response to the start of processing by the first encryption section (see responses to claim 3 and 4).

10.5. As per claim 7, Ishibashi is directed to a copyright protection system according to claim 3, wherein the first and second time-varying key generation sections generate the time-varying key based on the first and second random numbers and the common key (time varying keys, and their generation is disclosed in method ISO/IEC 9798-3 for mutual authentication. See column 7 line 37).

10.6. As per claim 8, Ishibashi is directed to a copyright protection system according to claim 3, wherein the first and second contents key generation sections generate the contents key based on the second decryption limitation and the time-varying key (see response to claims 45 and 5).

10.7. As per claim 9, Ishibashi is directed to a copyright protection system according to claim 3, wherein the encryption device and the decryption device further include respective first and second data sequence key generation sections for generating a data sequence key based on a data sequence input to or output from the encryption device and the decryption device, and wherein the first and second time-varying key generation sections generate the time-varying key based on the first and second random numbers and the respective data sequence key(as described in column 13 lines 57 to 60 and column 14 lines 22 to 24, alternative and more comprehensive methods to secure the exchange of keys between the parties may be deployed. Sequence key generation is a well-known method to synchronize receiver and transmitter engaged in secure data transmission and improve the strength of encryption, as described in text books such as Bruce Schneier's Applied Cryptography, ISBN 0-471-11709-9, (see section 9.5). Ishibashi's disclosure of mutual authentication implies use of well-known methods to perform mutual authentication, such as sequence key generation).

10.8. As per claim 10, 11, 12 Ishibashi is directed to a copyright protection system according to claim 3, wherein the encryption device and the decryption device further include respective first and second data sequence key generation sections for generating a data sequence key based on a data sequence input to or output from the encryption device and the decryption device, and wherein the first and second time-varying key generation sections generate the time-varying key based on the first and second random numbers, the common key, and the respective data sequence key (see response to claims 9, 3 and 4).

10.9. As per claim 13, Ishibashi is directed to a copyright protection system according to claim 3, wherein the first and second mutual authentication sections mutually authenticate the decryption device and the encryption device, respectively, by communication in accordance with a challenge-response type authentication protocol (as described in column 13 lines 57 to 60 and column 14 lines 22 to 24, alternative and more comprehensive methods to secure the exchange of keys between the parties may be deployed. Challenge-response is a well-known method to establish mutual authentication between parties, as described in text books such as Bruce Schneier's Applied Cryptography, ISBN 0-471-11709-9, (see section 3.2, page 54). Ishibashi's disclosure of mutual authentication implies use of well-known methods to perform mutual authentication, such as sequence key generation).

10.11. As per claim 14, Ishibashi is directed to an encryption device for performing cryptographic communication in association with a decryption device using a contents key, comprising: a contents storage section for storing contents (fig. 8 item 11); a second encryption section for encrypting the first decryption limitation using a time-varying key and outputting the second encrypted decryption limitation to the decryption device (see response to claim 1); a contents key generation section (item 14) for generating the contents key based on a second decryption limitation obtained by updating a first decryption limitation (column 6 lines 1 to 20, column 10 lines 53 to 66, and column 12 lines 25 to 44 disclose Ishibashi's use of SCMS, which controls the number of copies made from copyright protected material by updating limitations of copy codes in the content data and keys); and a first encryption section for encrypting the contents using the contents key and outputting the encrypted contents (item 16).

10.12. As per claims 15 to 25 Ishibashi is directed to an encryption device according to claim 14 (item 100 in Fig. 8 discloses both encryption and decryption devices, as it receives the encrypted content data from item 10, decrypts it to extract the content, and re-encrypts it in accordance with the copy control code (copy limitation) and sends it to item 200 (another Information Center), which perform decryption. As described in responses to claims 1 to 13, this process is secured by mutual authentication between items 10, 100, 200 and other elements in Fig. 8. Mutual authentication involves the use of encryption techniques such as time-varying keys, random number generation and use for

key generation, challenge–response protocol, data segmentation, etc. Ishibashi also discloses SCMS method for copy control. In the following, the encryption device is disclosed by item 100, and decryption device is disclosed by item 200. Item 100 does disclose all the elements of claim 14, as it includes and encryption section, and performs SCMS to update the copy code sent to item 200), further including a decryption section for decrypting the first encrypted decryption limitation transferred from the decryption device (item 131) using the time-varying key to generate the second decryption limitation, and the contents key generation section generates the contents key based on the second decryption limitation generated by the decryption device (item 133 and the associated text, also see responses to claims 1 to 14).

10.13. As per claim 26, Ishibashi is directed to a decryption device (Fig. 8 item 100 or 200) for performing cryptographic communication in association with an encryption device (item 100 or 10) using a contents key, comprising: a second decryption section for decrypting a second encrypted decryption limitation transferred from the encryption device using the time-varying key and outputting a first decryption limitation (see response to claim 1); a decryption limitation updating section for updating a first decryption limitation to a second decryption limitation in accordance with a decryption limitation updating rule (the copy control mechanism as discussed in claim 1 in item 200, which performs SMCS protocol which includes updating a copy code, as described in column 6 line 1 to 20); a contents key generation section for generating the contents key from a

second decryption limitation (item 231 generates the key to decrypt the content decryption key, which in accordance with SMCS includes a copy code (decryption limitation); and a first decryption section for decrypting encrypted contents using the contents key generated by the contents key generation section (item 236 and the associated text).

10.14. As per claims 27 to 36 Ishibashi is directed to a decryption device according to claim 26, further including an encryption section for encrypting the second decryption limitation using a time-varying key, and outputting the first encrypted decryption limitation (item 200 performs SMCS protocol which includes updating a copy code, as described in column 6 line 1 to 20).

10.15. As per claims 37 to 47, Ishibashi is directed to a recording medium storing a program for use in causing a computer to perform cryptographic communication with an encryption device (Fig. 8 item 100), a second decryption section for decrypting a second encrypted decryption limitation transferred from the encryption device using the time-varying key and outputting a first decryption limitation (see response to claim 1); a decryption limitation updating section for updating a first decryption limitation to a second decryption limitation in accordance with a decryption limitation updating rule (the copy control mechanism as discussed in claim 1 in item 200, which performs SMCS protocol which includes updating a copy code, as described in column 6 line 1 to 20); using a contents key, wherein: the program causes the computer to function as:

a contents key generation section for generating the contents key from a second decryption limitation (item 133, as described in response to claim 15); and a first decryption section for decrypting encrypted contents using the contents key generated by the contents key generation section (item 131 as explained in response to claim 15, and response to claims 1 to 16).

10.16. As per claim 48, Ishibashi is directed to a copyright protection system according to claim 1, wherein the first and second contents key generation sections generate the contents key by using an algorithm which uses the second decryption limitation as an input (as discussed in the Response to Arguments section above, Ishibashi teaches a key ($K_{cd}{}^{cx}$), which is an encryption key generated based on the copy control code (second decryption limitation). Therefore the content key generator generates the key with the second decryption limitation as an input).

10.17 As per claim 49, Ishibashi is directed to a copyright protection system according to claim 48, but Ishibashi does not disclose details such as the encryption technique to be used to perform different encryption processes, as the details of many encryption algorithms and techniques were well known in art at the time of his invention. Therefore, Ishibashi does not explicitly specify the one-way function as the algorithm to perform encryption.

Examiner takes the official notice that One-way function was a well known and widely practiced encryption technique at the time of invention. Therefore, it would have been obvious to the one skilled in art to use the One-way function as the algorithm to generate the key. The motivation to do so would have been to protect the key generation algorithm by using a one-way function, which makes it difficult for the hackers to discover the elements of the key generation process by analyzing the key.

As an example of prior art, please see Applied Cryptography (as identified in response to claim 9) sections 2.4 and 8.1.

10.18 The requirements of claim 50 are substantially similar to the requirements of claims 2-16 above.

Conclusion

11. **THIS ACTION IS MADE FINAL**. See MPEP § 7.39. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory

action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is (571) 272-3739. The examiner can be normally reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on (571) 272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Farid Homayounmehr

8/14/2008

/Kristine Kincaid/

Supervisory Patent Examiner, Art Unit 2139